

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	8	(non adj orthogonal non-orthogonal) and von adj neumann	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2007/05/10 13:36
L2	2	(non adj orthogonal non-orthogonal) with sets and von adj neumann	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2007/05/10 13:35
L3	3	("5819242" "5971579" "6317766").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2007/05/10 13:36
S1	0	Gisin.in. and quantum adj cryptopgraphy	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2007/05/07 12:55
S2	0	Acin.in. and quantum adj cryptopgraphy	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2006/11/21 12:01
S3	0	nicolas.in. and quantum adj cryptopgraphy	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2006/11/21 12:01
S4	0	scarani.in. and quantum adj cryptopgraphy	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2006/11/21 12:01
S5	0	ribordy.in. and quantum adj cryptopgraphy	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2006/11/21 12:02
S6	0	quantum adj cryptopgraphy and @ad<="20021115"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2006/11/21 12:48
S7	218	quantum adj cryptography and @ad<="20021115"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2006/11/21 11:07

EAST Search History

S8	5	quantum adj cryptography and von adj neumann and @ad<="20021115"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2006/11/21 11:08
S9	13	Gisin.in. and quantum adj cryptography	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2006/11/21 12:02
S10	3	Acin.in. and quantum adj cryptography	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2006/11/21 12:09
S11	10	nicolas.in. and quantum adj cryptography	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2006/11/21 12:09
S12	3	scarani.in. and quantum adj cryptography	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2006/11/21 12:47
S13	7	ribordy.in. and quantum adj cryptography	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2006/11/21 12:47
S14	21	quantum adj cryptography and ("non-orthogonal" non adj orthogonal) and @ad<="20021115"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2006/11/21 12:51
S15	21	quantum adj cryptography and ("non-orthogonal" non adj orthogonal) and (encod\$3 encrypt\$3 encipher\$3 scrambl\$3) and @ad<="20021115"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2006/11/21 12:54
S16	11	quantum adj cryptography and ("non-orthogonal" non adj orthogonal) and (encod\$3 encrypt\$3 encipher\$3 scrambl\$3) with random and @ad<="20021115"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2006/11/21 15:10

EAST Search History

S17	79	380/256.ccls.and @ad<="20021115"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2006/11/21 15:10
S18	31	380/256.ccls. and quantum and @ad<="20021115"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2006/11/21 15:11
S19	15	380/256.ccls. and quantum and non adj orthogonal and @ad<="20021115"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2006/11/21 15:11
S20	490	quantum adj cryptography	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2007/05/07 15:24
S21	4	quantum adj cryptography and photon adj number adj splitting	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2007/05/07 13:27
S26	128	380/256.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2007/05/07 17:12
S27	64	380/256.ccls. and quantum	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2007/05/08 09:33
S28	57	380/256.ccls. and quantum and channel\$1	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2007/05/07 17:14
S29	26	380/256.ccls. and quantum and (quantum and (public convention\$2)) adj channel\$1	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2007/05/07 17:15
S30	26	380/256.ccls. and quantum and (quantum and (public convention\$2)) adj channel\$1 and bit\$1	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2007/05/08 09:19

EAST Search History

S31	2	"6990583"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2007/05/08 09:20
S32	25	380/256.ccls. and (non adj orthogonal non-orthogonal)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2007/05/08 09:43
S33	11	"6028935"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2007/05/08 09:39
S34	2	380/256.ccls. and (non adj orthogonal non-orthogonal) and von adj neumann	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2007/05/10 13:35
S35	4	380/256.ccls. and (non adj orthogonal non-orthogonal) with set\$1	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2007/05/08 09:50
S36	5	380/256.ccls. and bit\$1 with quantum with set\$1	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2007/05/08 09:54
S37	139	bit\$1 with quantum with set\$1	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2007/05/08 09:54
S38	8	bit\$1 with quantum with set\$1 and non adj orthogonal	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT	OR	OFF	2007/05/08 09:55

[Sign in](#)[Web](#) [Images](#) [Video](#) [News](#) [Maps](#) [more »](#)

quantum cryptography non-orthogonal

[Search Patents](#)[Advanced Patent Search](#)
[Google Patent Search](#)

Patents

Patents 1 - 10 on quantum cryptography non-orthogonal. (0.11 seconds)

Quantum key distribution using non-orthogonal macroscopic signals

US Pat. 5515438 - Filed Nov 24, 1993 - International Business Machines Corporation

QUANTUM KEY DISTRIBUTION USING NON-ORTHOGONAL MACROSCOPIC SIGNALS DESCRIPTION 1.

... "Quantum Cryptography Using any Two Non-orthogonal States" Phys. Rev. ...

Quantum cryptography

US Pat. 5953421 - Filed Jan 30, 1997 - British Telecommunications public limited company

As further described below, the present invention can be used to enhance

significantly **quantum cryptography** using two **non-orthogonal** states. ...

Free-space quantum cryptography system

US Pat. 6289104 - Filed Aug 7, 1998 - Illinois Institute of Technology

As in the case The method for **quantum** key delivery in a single-photon, ...

retardation plate **non-orthogonal** transmitter basis systems through a trans- 41a, ...

Positive-operator-valued-measure receiver for quantum cryptography

US Pat. 5999285 - Filed May 23, 1997 - The United States of America as represented by the Secretary of the Army

7,1999 OTHER PUBLICATIONS Unambiguous Quantum Measurement of ... [57] ABSTRACT

Quantum key distribution (QKD) employs **non-orthogonal quantum** states to ...

Method and apparatus for quantum distribution of an encryption key

US Pat. 6272224 - Filed Apr 21, 1998 - France Telecom

This protocol was suggested by SJD PHOENIX and PD TOWNSEND in an article entitled "Quantum Cryptography and Secure Optical Communications" published in the ...

Quantum key distribution method and apparatus

US Pat. 6678379 - Filed Jun 18, 1999 - NEC Corporation

Field of the Invention The present invention relates generally to **quantum** **cryptography** techniques and, more particularly, to a method for testing the ...

Cryptographic key distribution method and apparatus thereof

US Pat. 6895092 - Filed Aug 21, 2001 - NEC Corporation

In this Letters, a method used the two **non-orthogonal** states being suitable for the transmission by optical fibers is described. At the **quantum cryptography** ...

Secure communications with low-orbit spacecraft using quantum cryptography

US Pat. 5966224 - Filed May 20, 1997 - The Regents of the University of California

Quantum cryptography avoids the cumbersome physical security aspects of ... a secure ground station utilizing **quantum cryptography** based on **non-orthogonal** ...

Method for key distribution using quantum cryptography

US Pat. 5764765 - Filed Apr 22, 1996 - British Telecommunications public limited company CH Bennett, "Quantum Cryptography Using any Two Non-Orthogonal States", Physical

Review Letters, 68 3121 (1992). 9. SM Barnett and SJD Phoenix. ...

Temperature compensation for QKD systems

US Pat. 7102121 - Filed Jun 29, 2004 - MagiQ Technologies, Inc.

The general principles of **quantum cryptography** were first set forth by Bennett and Brassard in ... **Non-Orthogonal States**", Phys. Rev. Lett. 68 3121 (1992). ...

Google ►

Result Page: 1 2 [Next](#)

[Search Patents](#)

[Google Patent Search Help](#) | [Advanced Patent Search](#)

[Google Home](#) - [About Google](#) - [About Google Patent Search](#)

©2007 Google

[Sign in](#)[Web](#) [Images](#) [Video](#) [News](#) [Maps](#) [more »](#)

quantum cryptography non-orthogonal

[Search Patents](#)[Advanced Patent Search](#)
[Google Patent Search](#)

Patents

Patents 11 - 13 on quantum cryptography non-orthogonal. (0.02 seconds)

Cryptographic receiver

US Pat. 6028935 - Filed Apr 10, 1996 - The Secretary of State for Defence in Her Britannic Majesty's Government of the United Kingdom of Great Britain and Northern Ireland

OTHER PUBLICATIONS Bennett, Charles H., "Quantum Cryptography Using Any Two ...

The filters (22, 24) impose **non-orthogonal** measurement bases on photons ...

Key bank systems and methods for QKD

US Pat. 7181011 - Filed May 24, 2004 - MagiQ Technologies, Inc.

The general principles of **quantum cryptography** were first set forth by Bennett and ... "Quantum Cryptography Using Any Two Non- Orthogonal States", Phys. ...

Quantum cryptographic system with reduced data loss

US Pat. 5732139 - Filed Aug 26, 1996

For a typical $e=0.1$, "Quantum Cryptography Using Any Two Non-orthogonal" the latter is 18% and the fraction of accepted data is 82%. ...

Result Page: [Previous](#) [1](#) [2](#)

quantum cryptography non-orthogonal

[Search Patents](#)[Google Patent Search Help](#) | [Advanced Patent Search](#)[Google Home](#) - [About Google](#) - [About Google Patent Search](#)

©2007 Google


[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)
 The ACM Digital Library The Guide

 quantum cryptography non-orthogonal

[Feedback](#) [Report a problem](#) [Satisfaction survey](#)

 Terms used [quantum cryptography non orthogonal](#)

 Found **391 of 201,062**

Sort results by

 [Save results to a Binder](#)
[Try an Advanced Search](#)

Display results

 [Search Tips](#)
[Try this search in The ACM Guide](#)
 [Open results in a new window](#)

Results 1 - 20 of 200

 Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

Best 200 shown

Relevance scale

1 [Quantum rendering: an introduction to quantum computing and quantum algorithms, and their applications to computer graphics: Quantum rendering: an introduction to quantum computing, quantum algorithms and their applications to computer graphics](#)
 Marco Lanza, Jeffrey Uhlmann
 July 2005 **ACM SIGGRAPH 2005 Courses SIGGRAPH '05**
Publisher: ACM Press
 Full text available: [pdf\(942.06 KB\)](#) Additional Information: [full citation](#)

2 [Quantum information processing: Incremental information extraction from Grover's algorithm](#)

Bryan C. Jacobs, Todd B. Pittman, James D. Franson
 January 2004 **Proceedings of the winter international symposium on Information and communication technologies WISICT '04**

Publisher: Trinity College Dublin

Full text available: [pdf\(54.01 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#)

The iterative nature of Grover's quantum search algorithm may limit the feasibility of its implementation on quantum computers having relatively short coherence times. It may be possible to make a parallel version of the algorithm by extracting partial information about the solution after a limited number of iterations. Here we investigate the use of positive operator value measurements to reduce the coherence time requirements of Grover's algorithm. The utilization of single qubit measurements ...

3 [Contributed session 3: Knowledge in quantum systems](#)

R. van der Meyden, Manas Patra
 June 2003 **Proceedings of the 9th conference on Theoretical aspects of rationality and knowledge TARK '03**

Publisher: ACM Press

Full text available: [pdf\(1.09 MB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

This paper applies to quantum systems a modelling for the logic of knowledge, originally developed for reasoning about distributed systems, but since then applied to game theory, computer security and artificial intelligence. A formal model of quantum message passing systems is developed and the question of how one might define the semantics of a modal operator for knowledge in this model is considered. It is argued that there are at

least two plausible semantics, depending on whether the agents ...

4 Miscellany: Quantum cryptography in practice

 Chip Elliott, David Pearson, Gregory Troxel

August 2003 **Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications SIGCOMM '03**

Publisher: ACM Press

Full text available:  [pdf\(809.93 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

BBN, Harvard, and Boston University are building the DARPA Quantum Network, the world's first network that delivers end-to-end network security via high-speed Quantum Key Distribution, and testing that Network against sophisticated eavesdropping attacks. The first network link has been up and steadily operational in our laboratory since December 2002. It provides a Virtual Private Network between private enclaves, with user traffic protected by a weak-coherent implementation of quantum cryptogra ...

Keywords: IPsec, cryptographic protocols, error correction, key agreement protocols, privacy amplification, quantum cryptography, quantum key distribution, secure networks

5 Quantum rendering: an introduction to quantum computing and quantum algorithms, and their applications to computer graphics: Hybrid quantum-classical computing with applications to computer graphics

 Marco Lanza, Jeffrey K. Uhlmann

July 2005 **ACM SIGGRAPH 2005 Courses SIGGRAPH '05**

Publisher: ACM Press

Full text available:  [pdf\(390.33 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#)

Quantum computing (QC) has become an important area of research in computer science because of its potential to provide more efficient algorithmic solutions to certain problems than are possible with classical computing (CC). In particular, QC is able to exploit the special properties of quantum superposition to achieve computational parallelism beyond what can be achieved with parallel CC computers. However, these special properties are not applicable for general computation. Therefore, we prop ...

Keywords: collision detection, computational geometry, computer graphics, databases, grover's algorithm, quantum algorithms, quantum cloning, quantum computing, simulation, state estimation, virtual reality

6 25 years of quantum cryptography

 Gilles Brassard, Claude Crépeau

September 1996 **ACM SIGACT News**, Volume 27 Issue 3

Publisher: ACM Press

Full text available:  [pdf\(918.87 KB\)](#) Additional Information: [full citation](#), [abstract](#), [citations](#), [index terms](#)

The fates of *SIGACT News* and Quantum Cryptography are inseparably entangled. The exact date of Stephen Wiesner's invention of "conjugate coding" is unknown but it cannot be far from April 1969, when the premier issue of *SIGACT News*---or rather *SICACT News* as it was known at the time---came out. Much later, it was in *SIGACT News* that Wiesner's paper finally appeared [74] in the wake of the first author's early collaboration with Charles H. Bennett [7]. It was also in < ...

7 Unconditional security in quantum cryptography

Dominic Mayers

May 2001 **Journal of the ACM (JACM)**, Volume 48 Issue 3

Publisher: ACM Press

Full text available:  pdf(394.84 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)

Basic techniques to prove the unconditional security of quantum cryptography are described. They are applied to a quantum key distribution protocol proposed by Bennett and Brassard [1984]. The proof considers a practical variation on the protocol in which the channel is noisy and photons may be lost during the transmission. Each individual signal sent into the channel must contain a single photon or any two-dimensional system in the exact state described in the protocol. No restriction is i ...

Keywords: quantum cryptography, quantum information theory, unconditional security

8 An introduction to quantum cryptography

 Nick Papanikolaou

May 2005 **Crossroads**, Volume 11 Issue 3

Publisher: ACM Press

Full text available:  html(40.57 KB) Additional Information: [full citation](#), [references](#), [index terms](#)



9 Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working]

 C. H. Bennett, G. Brassard

November 1989 **ACM SIGACT News**, Volume 20 Issue 4

Publisher: ACM Press

Full text available:  pdf(381.62 KB) Additional Information: [full citation](#), [citations](#), [index terms](#)



10 Quantum computing: the end of classical cryptography?

 Gilles Brassard

December 1994 **ACM SIGACT News**, Volume 25 Issue 4

Publisher: ACM Press

Full text available:  pdf(512.72 KB) Additional Information: [full citation](#), [index terms](#)



11 Special section on impact of quantum technologies on networks and networking

 research: Quantum networks: from quantum cryptography to quantum architecture

Tatjana Curcic, Mark E. Filippowski, Almadena Chtchelkanova, Philip A. D'Ambrosio, Stuart A. Wolf, Michael Foster, Douglas Cochran

October 2004 **ACM SIGCOMM Computer Communication Review**, Volume 34 Issue 5

Publisher: ACM Press

Full text available:  pdf(221.26 KB) Additional Information: [full citation](#), [abstract](#), [references](#)



As classical information technology approaches limits of size and functionality, practitioners are searching for new paradigms for the distribution and processing of information. Our goal in this Introduction is to provide a broad view of the beginning of a new era in information technology, an era of quantum information, where previously underutilized quantum effects, such as quantum superposition and entanglement, are employed as resources for information encoding and processing. The ability t

12 Regular features: Review of "The code book: the evolution of secrecy from Mary

◆ Queen of Scots to quantum cryptography" by Simon Singh. Anchor Books.

Jim Reeds

June 2001 **ACM SIGACT News**, Volume 32 Issue 2

Publisher: ACM Press

Full text available:  [pdf\(540.02 KB\)](#) Additional Information: [full citation](#)

13 A proof of the security of quantum key distribution (extended abstract)

◆ **Eli Biham, Michel Boyer, P. Oscar Boykin, Tal Moran, Vwani Roychowdhury**

May 2000 **Proceedings of the thirty-second annual ACM symposium on Theory of computing STOC '00**

Publisher: ACM Press

Full text available:  [pdf\(968.70 KB\)](#) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

14 Special section on impact of quantum technologies on networks and networking

◆ research: Quantum-noise: protected data encryption for WDM fiber-optic networks

Eric Corndorf, Chuang Liang, Gregory S. Kanter, Prem Kumar, Horace P. Yuen

October 2004 **ACM SIGCOMM Computer Communication Review**, Volume 34 Issue 5

Publisher: ACM Press

Full text available:  [pdf\(696.74 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

We demonstrate high data-rate quantum-noise-protected data encryption through optical fibers using coherent states of light. Specifically, we demonstrate 650Mbps data encryption through a 10Gbps data-bearing, in-line amplified 200km-long line. In our protocol, legitimate users (who share a short secret-key) communicate using an M-ary signal set while an attacker (who does not share the secret-key) is forced to contend with the fundamental and irreducible quantum-measurement noise of coherent stat ...

Keywords: data encryption, quantum cryptography

15 An introduction to quantum computing for non-physicists

◆ **September 2000 ACM Computing Surveys (CSUR)**, Volume 32 Issue 3

Publisher: ACM Press

Full text available:  [pdf\(491.89 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)

Richard Feynman's observation that certain quantum mechanical effects cannot be simulated efficiently on a computer led to speculation that computation in general could be done more efficiently if it used these quantum effects. This speculation proved justified when Peter Shor described a polynomial time quantum algorithm for factoring integers. In quantum systems, the computational space increases exponentially with the size of the system, which enables exponential parallelism. ...

Keywords: complexity, parallelism, quantum computing

16 Security of quantum protocols against coherent measurements

◆ **Andrew Chi-Chih Yao**

May 1995 **Proceedings of the twenty-seventh annual ACM symposium on Theory of computing STOC '95**

Publisher: ACM Press

Full text available:  [pdf\(668.31 KB\)](#) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

17 Networking and mobile computing: A quantum no-key protocol for secure data communication

 Yoshito Kanamori, Seong-Moo Yoo, Mohammad Al-Shurman
March 2005 **Proceedings of the 43rd annual Southeast regional conference - Volume 2 ACM-SE 43**

Publisher: ACM Press

Full text available:  [pdf\(340.64 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#)

Since classical cryptography relies on difficulty and infeasibility of computation to find the plain text, the cryptography is losing security more and more as computational power is increased by technical innovations. Therefore, unconditionally secure cryptography has been expected. In this paper, we propose a novel, secure, no-key, protocol: Quantum Three-Pass Protocol (QTPP). In this protocol, quantum superposition states are used for transmission instead of classical signals in classical cry ...

18 Some facets of complexity theory and cryptography: A five-lecture tutorial

 Jörg Rothe
December 2002 **ACM Computing Surveys (CSUR)**, Volume 34 Issue 4

Publisher: ACM Press

Full text available:  [pdf\(2.78 MB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#), [review](#)

In this tutorial, selected topics of cryptology and of computational complexity theory are presented. We give a brief overview of the history and the foundations of classical cryptography, and then move on to modern public-key cryptography. Particular attention is paid to cryptographic protocols and the problem of constructing key components of protocols such as one-way functions. A function is one-way if it is easy to compute, but hard to invert. We discuss the notion of one-way functions both ...

Keywords: Complexity theory, interactive proof systems, one-way functions, public-key cryptography, zero-knowledge protocols

19 Communicating quantum processes

 Simon J. Gay, Rajagopal Nagarajan
January 2005 **ACM SIGPLAN Notices , Proceedings of the 32nd ACM SIGPLAN-SIGACT symposium on Principles of programming languages POPL '05**, Volume 40 Issue 1

Publisher: ACM Press

Full text available:  [pdf\(247.88 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

We define a language CQP (Communicating Quantum Processes) for modelling systems which combine quantum and classical communication and computation. CQP combines the communication primitives of the pi-calculus with primitives for measurement and transformation of quantum state; in particular, quantum bits (qubits) can be transmitted from process to process along communication channels. CQP has a static type system which classifies channels, distinguishes between quantum and classical data, and co ...

Keywords: formal language, quantum communication, quantum computing, semantics, types, verification

20 Session 10B: Secure multi-party quantum computation

Claude Crépeau, Daniel Gottesman, Adam Smith

May 2002 **Proceedings of the thiry-fourth annual ACM symposium on Theory of computing STOC '02**

Publisher: ACM Press

Full text available: [pdf\(236.21 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Secure multi-party computing, also called *secure function evaluation*, has been extensively studied in classical cryptography. We consider the extension of this task to computation with quantum inputs and circuits. Our protocols are information-theoretically secure, i.e. no assumptions are made on the computational power of the adversary. For the weaker task of *verifiable quantum secret sharing*, we give a protocol which tolerates any $t \leq n/4$ cheating parties ...

Keywords: distributed computing, multi-party protocols, quantum cryptography, secure function evaluation

Results 1 - 20 of 200

Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2007 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads: [Adobe Acrobat](#) [QuickTime](#) [Windows Media Player](#) [Real Player](#)

Dialog DataStar

[options](#)[logoff](#)[feedback](#)[help](#)[databases](#)[easy search](#)

Advanced Search:

Inspec - 1898 to date (INZZ)

[limit](#)

Search history:

No.	Database	Search term	Info added since	Results	
CP		[Clipboard]	-	0	-
1	INZZ	quantum ADJ cryptography ADJ non-orthogonal	unrestricted	0	-

[hide](#) | [delete all search steps...](#) | [delete individual search steps...](#)

Enter your search term(s): [Search tips](#) Thesaurus mapping

whole document



[search](#)

Information added since: or:

Images

Select special search terms from the following list(s):

- Publication year 1950-
- Publication year 1898-1949
- Inspec thesaurus - browse headings
- Inspec thesaurus - enter a term
- Classification codes A: Physics, 0-1
- Classification codes A: Physics, 2-3
- Classification codes A: Physics, 4-5
- Classification codes A: Physics, 6
- Classification codes A: Physics, 7
- Classification codes A: Physics, 8
- Classification codes A: Physics, 9
- Classification codes B: Electrical & Electronics, 0-5

-  Classification codes B: Electrical & Electronics, 6-9
-  Classification codes C: Computer & Control
-  Classification codes D: Information Technology
-  Classification codes E: Mech., Manufac. & Production Engineering
-  Treatment codes
-  Inspec sub-file
-  Language of publication
-  Publication types

[Top](#) - [News & FAQS](#) - [Dialog](#)

© **2007** Dialog


[Home](#) | [Login](#) | [Logout](#) | [Access Information](#) | [Alerts](#) |

Welcome United States Patent and Trademark Office

 [Search Results](#)[BROWSE](#)[SEARCH](#)[IEEE Xplore GUIDE](#)

Results for "((quantum cryptography)<in>metadata) and sets and orthogonal"

[e-mail](#)Your search matched **46** of **1566306** documents.A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.» [Search Options](#)[View Session History](#)[New Search](#)» [Key](#)

IEEE JNL IEEE Journal or Magazine

IET JNL IET Journal or Magazine

IEEE CNF IEEE Conference Proceeding

IET CNF IET Conference Proceeding

IEEE STD IEEE Standard

[Modify Search](#)

((quantum cryptography)<in>metadata) and sets and orthogonal

[Search](#) Check to search only within this results setDisplay Format: Citation Citation & Abstract[view selected items](#) [Select All](#) [Deselect All](#)

- 1. **An autocompensating fiber-optic quantum cryptography system based on splitting of light**
Bethune, D.S.; Risk, W.P.;
[Quantum Electronics, IEEE Journal of](#)
Volume 36, Issue 3, March 2000 Page(s):340 - 347
Digital Object Identifier 10.1109/3.825881
[AbstractPlus](#) | [References](#) | [Full Text: PDF\(216 KB\)](#) [IEEE JNL](#)
[Rights and Permissions](#)
- 2. **Square-root measurement for quantum symmetric mixed state signals**
Kato, K.; Hirota, O.;
[Information Theory, IEEE Transactions on](#)
Volume 49, Issue 12, Dec. 2003 Page(s):3312 - 3317
Digital Object Identifier 10.1109/TIT.2003.820050
[AbstractPlus](#) | [References](#) | [Full Text: PDF\(360 KB\)](#) [IEEE JNL](#)
[Rights and Permissions](#)
- 3. **Quantum cryptography with imperfect apparatus**
Mayers, D.; Yao, A.;
[Foundations of Computer Science, 1998. Proceedings. 39th Annual Symposium](#)
8-11 Nov. 1998 Page(s):503 - 509
Digital Object Identifier 10.1109/SFCS.1998.743501
[AbstractPlus](#) | [Full Text: PDF\(104 KB\)](#) [IEEE CNF](#)
[Rights and Permissions](#)
- 4. **Controllability, observability, and parameter identification of two coupled**
D'Alessandro, D.;
[Automatic Control, IEEE Transactions on](#)
Volume 50, Issue 7, July 2005 Page(s):1054 - 1058
Digital Object Identifier 10.1109/TAC.2005.851460
[AbstractPlus](#) | [Full Text: PDF\(216 KB\)](#) [IEEE JNL](#)
[Rights and Permissions](#)
- 5. **Quantum information theory**
Bennett, C.H.; Shor, P.W.;
[Information Theory, IEEE Transactions on](#)
Volume 44, Issue 6, Oct. 1998 Page(s):2724 - 2742
Digital Object Identifier 10.1109/18.720553

[AbstractPlus](#) | [References](#) | [Full Text: PDF\(468 KB\)](#) | [IEEE JNL](#)
[Rights and Permissions](#)

6. Quantum cryptography for secure satellite communications

Hughes, R.J.; Buttler, W.T.; Kwiat, P.G.; Lamoreux, S.K.; Morgan, G.L.; Nordl Peterson, C.G.;
[Aerospace Conference Proceedings, 2000 IEEE](#)
Volume 1, 18-25 March 2000 Page(s):191 - 200 vol.1
Digital Object Identifier 10.1109/AERO.2000.879387

[AbstractPlus](#) | [Full Text: PDF\(876 KB\)](#) | [IEEE CNF](#)
[Rights and Permissions](#)

7. Quantum information processing: cryptography, computation, and telep

Spiller, T.P.;
[Proceedings of the IEEE](#)
Volume 84, Issue 12, Dec. 1996 Page(s):1719 - 1746
Digital Object Identifier 10.1109/5.546399

[AbstractPlus](#) | [References](#) | [Full Text: PDF\(3192 KB\)](#) | [IEEE JNL](#)
[Rights and Permissions](#)

8. Integrated-optical realizations of quantum key distribution over maximall bases

Nazarathy, M.; Tselniker, I.; Regev, Y.; Orenstein, M.; Katz, M.;
[Selected Topics in Quantum Electronics, IEEE Journal of](#)
Volume 12, Issue 4, July-Aug. 2006 Page(s):897 - 913
Digital Object Identifier 10.1109/JSTQE.2006.876175

[AbstractPlus](#) | [Full Text: PDF\(360 KB\)](#) | [IEEE JNL](#)
[Rights and Permissions](#)

9. Cryptographic distinguishability measures for quantum-mechanical state

Fuchs, C.A.; van de Graaf, J.;
[Information Theory, IEEE Transactions on](#)
Volume 45, Issue 4, May 1999 Page(s):1216 - 1227
Digital Object Identifier 10.1109/18.761271

[AbstractPlus](#) | [References](#) | [Full Text: PDF\(260 KB\)](#) | [IEEE JNL](#)
[Rights and Permissions](#)

10. Secure key exchange over 1.9 km free-space range using quantum crypt

Rarity, J.G.; Gorman, P.M.; Tapster, P.R.;
[Electronics Letters](#)
Volume 37, Issue 8, 12 Apr 2001 Page(s):512 - 514
Digital Object Identifier 10.1049/el:20010334

[AbstractPlus](#) | [Full Text: PDF\(356 KB\)](#) | [IET JNL](#)

11. On quantum authentication protocols

Kanamori, Y.; Seong-Moo Yoo; Gregory, D.A.; Sheldon, F.T.;
[Global Telecommunications Conference, 2005. GLOBECOM '05. IEEE](#)
Volume 3, 28 Nov.-2 Dec. 2005 Page(s):5 pp.
Digital Object Identifier 10.1109/GLOCOM.2005.1577930

[AbstractPlus](#) | [Full Text: PDF\(191 KB\)](#) | [IEEE CNF](#)
[Rights and Permissions](#)

12. Quantum information processing: basic ideas, implementations, and pos communications

Karlsson, A.;
[Integrated Optics and Optical Fibre Communications, 11th International Confe](#)
[23rd European Conference on Optical Communications \(Conf. Publ. No.: 448\)](#)
Volume 2, 22-25 Sept. 1997 Page(s):237 - 240 vol.2

[AbstractPlus](#) | Full Text: [PDF\(484 KB\)](#) IET CNF

13. Making unbreakable code
Mullins, J.;
[Spectrum, IEEE](#)
Volume 39, Issue 5, May 2002 Page(s):40 - 45
Digital Object Identifier 10.1109/6.999793
[AbstractPlus](#) | Full Text: [PDF\(251 KB\)](#) | Full Text: [HTML](#) IEEE JNL
[Rights and Permissions](#)

14. Optoelectronic quantum telecommunications based on spins in semiconductors
Yablonovitch, E.; Jiang, H.W.; Kosaka, H.; Robinson, H.D.; Rao, D.S.; Szkopek, J.;
[Proceedings of the IEEE](#)
Volume 91, Issue 5, May 2003 Page(s):761 - 780
Digital Object Identifier 10.1109/JPROC.2003.811799
[AbstractPlus](#) | References | Full Text: [PDF\(1738 KB\)](#) | Full Text: [HTML](#) IEEE JNL
[Rights and Permissions](#)

15. A short wavelength GigaHertz clocked fiber-optic quantum key distribution
Gordon, K.J.; Fernandez, V.; Townsend, P.D.; Buller, G.S.;
[Quantum Electronics, IEEE Journal of](#)
Volume 40, Issue 7, July 2004 Page(s):900 - 908
Digital Object Identifier 10.1109/JQE.2004.830182
[AbstractPlus](#) | References | Full Text: [PDF\(344 KB\)](#) IEEE JNL
[Rights and Permissions](#)

16. Experimental multiuser quantum key distribution network using a wavelength bus architecture
Kumavor, P.D.; Beal, A.C.; Donkor, E.; Wang, B.C.;
[Lightwave Technology, Journal of](#)
Volume 24, Issue 8, Aug. 2006 Page(s):3103 - 3106
Digital Object Identifier 10.1109/JLT.2006.878289
[AbstractPlus](#) | Full Text: [PDF\(144 KB\)](#) IEEE JNL
[Rights and Permissions](#)

17. On the power of quantum memory
Konig, R.; Maurer, U.; Renner, R.;
[Information Theory, IEEE Transactions on](#)
Volume 51, Issue 7, July 2005 Page(s):2391 - 2401
Digital Object Identifier 10.1109/TIT.2005.850087
[AbstractPlus](#) | References | Full Text: [PDF\(368 KB\)](#) IEEE JNL
[Rights and Permissions](#)

18. Generalized privacy amplification
Bennett, C.H.; Brassard, G.; Crepeau, C.; Maurer, U.M.;
[Information Theory, IEEE Transactions on](#)
Volume 41, Issue 6, Part 2, Nov. 1995 Page(s):1915 - 1923
Digital Object Identifier 10.1109/18.476316
[AbstractPlus](#) | Full Text: [PDF\(984 KB\)](#) IEEE JNL
[Rights and Permissions](#)

19. Quantum shadow enumerators
Rains, E.M.;
[Information Theory, IEEE Transactions on](#)
Volume 45, Issue 7, Nov. 1999 Page(s):2361 - 2366
Digital Object Identifier 10.1109/18.796376
[AbstractPlus](#) | References | Full Text: [PDF\(152 KB\)](#) IEEE JNL
[Rights and Permissions](#)

- 20. **Coding theorem and strong converse for quantum channels**
Winter, A.;
[Information Theory, IEEE Transactions on](#)
Volume 45, Issue 7, Nov. 1999 Page(s):2481 - 2485
Digital Object Identifier 10.1109/18.796385
[AbstractPlus](#) | [References](#) | Full Text: [PDF\(220 KB\)](#) | [IEEE JNL](#)
[Rights and Permissions](#)

- 21. **Upper bounds on the size of quantum codes**
Ashikhmin, A.; Litsyu, S.;
[Information Theory, IEEE Transactions on](#)
Volume 45, Issue 4, May 1999 Page(s):1206 - 1215
Digital Object Identifier 10.1109/18.761270
[AbstractPlus](#) | [References](#) | Full Text: [PDF\(248 KB\)](#) | [IEEE JNL](#)
[Rights and Permissions](#)

- 22. **Asymptotic redundancies for universal quantum coding**
Krattenthaler, C.; Slater, P.B.;
[Information Theory, IEEE Transactions on](#)
Volume 46, Issue 3, May 2000 Page(s):801 - 819
Digital Object Identifier 10.1109/18.841164
[AbstractPlus](#) | [References](#) | Full Text: [PDF\(536 KB\)](#) | [IEEE JNL](#)
[Rights and Permissions](#)

- 23. **Quantum error detection .II. Bounds**
Ashikhmin, A.E.; Barg, A.M.; Knill, E.; Litsyn, S.N.;
[Information Theory, IEEE Transactions on](#)
Volume 46, Issue 3, May 2000 Page(s):789 - 800
Digital Object Identifier 10.1109/18.841163
[AbstractPlus](#) | [References](#) | Full Text: [PDF\(364 KB\)](#) | [IEEE JNL](#)
[Rights and Permissions](#)

- 24. **Quantum error detection .I. Statement of the problem**
Ashikhmin, A.E.; Barg, A.M.; Knill, E.; Litsyn, S.N.;
[Information Theory, IEEE Transactions on](#)
Volume 46, Issue 3, May 2000 Page(s):778 - 788
Digital Object Identifier 10.1109/18.841162
[AbstractPlus](#) | [References](#) | Full Text: [PDF\(304 KB\)](#) | [IEEE JNL](#)
[Rights and Permissions](#)

- 25. **A quantum analog of Huffman coding**
Braunstein, S.L.; Fuchs, C.A.; Gottesman, D.; Hoi-Kwong Lo;
[Information Theory, IEEE Transactions on](#)
Volume 46, Issue 4, July 2000 Page(s):1644 - 1649
Digital Object Identifier 10.1109/18.850709
[AbstractPlus](#) | [References](#) | Full Text: [PDF\(176 KB\)](#) | [IEEE JNL](#)
[Rights and Permissions](#)